UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MARY YOON, et al.,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 24-cv-02612-NC

ORDER GRANTING JUDICIAL NOTICE; AND GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Re: ECF 24, 29, 31

This class action against Defendant Meta Platforms, Inc. brought by Plaintiffs Mary Yoon, William Martin, and Kat Walker arises from Meta's alleged collection of their sensitive video viewing data through tracking tools installed on third party websites. Plaintiffs bring several claims under the California Invasion of Privacy Act (CIPA). Defendant moves to dismiss these claims under Federal Rule of Civil Procedure 12(b)(6) and seeks judicial notice of 16 exhibits. For the following reasons, Defendant's motion to dismiss is GRANTED in part and DENIED in part, and the requests for judicial notice are GRANTED.

I. BACKGROUND

A. Factual Background

Plaintiffs' Complaint alleges the following facts.

1. Wiretapping Devices

Meta offers a suite of business tools, including Meta's pixel (Pixel), Facebook

SDK, and Conversions API.

The Pixel is an invisible web element that website owners can install on their websites to measure and track certain actions taken by users on their own websites. ECF 1-3 (FAC) ¶¶ 24–25. It is widely deployed across many industries. *Id.* ¶ 46. The Pixel collects a large range of user data. *Id.* ¶ 26. When a website user takes an action on a webpage which includes the Pixel, Meta's source code commands the user's device to re-direct the content of the communication to Meta while the exchange of the communication between the user and the website is still occurring. *Id.* ¶ 31. Through this technology, Meta intercepts each page a user visits, what buttons they click, and specific information they input into the website, along with a user's PII, like their IP address, allowing it to match its users with the data. *Id.* ¶¶ 33, 35. By design, Meta receives the contents of website communications as the website user enters the information, but before the website owner receives it. *Id.* ¶ 32. Meta falsely claims that it does not track non-Facebook user data; that data is still collected in dossiers called "shadow profiles." ¶ 40.

Facebook's other Business Tools function similarly. *Id.* ¶ 48. Advertisers can utilize the Facebook SDK for mobile applications to track events on their mobile apps. *Id.* Advertisers and web developers can also use the Conversions API to circumvent a user's choice to exercise privacy controls and collect server events that are linked to a Pixel ID. *Id.* ¶ 49. The Conversions API intercepts these communications contemporaneously and surreptitiously. *Id.*

Meta offers the Pixel to companies for free because it benefits Meta. *Id.* ¶ 43. Meta uses the data it gleans from tools like the Pixel to power its algorithms, providing it insight into the habits of users across the internet. *Id.* For example, it uses the data to target users with advertisements based on their interests and thus, increase its ad revenue. *Id.* ¶ 44. Thus, Meta intentionally obtained video viewing information due to its valuable advertising purposes because it can shed light on people's interests, politics, artistic tastes—it is not an accident, mistake, or inadvertence. *Id.* ¶¶ 87, 91. Meta knows about the data transmissions and does not make a genuine effort to prevent it; it wants to have

data transmissions to support its business model and advertising revenue. *Id.* ¶¶ 88–89, 91.

The Pixel and other business tools operate all the time and work the same way for everyone who visits a website with the tools installed. *Id.* ¶ 52.

2. Video Viewing Data

The Pixel and related business tools were installed on each of the subject websites when Plaintiffs watched video content on those sites. *Id.* ¶ 53. The subject websites include HGTV.com, Bloomberg.com, USAToday.com, 247Sports.com, and PBS.com. *Id.* ¶¶ 57–67. All host videos. *Id.* Using the Pixel and related business tools, these websites have been transmitting viewing history information to Meta. *Id.* ¶ 50.

Plaintiffs allege that each had their video viewing history unlawfully transmitted from the subject websites to Meta, which in turn was matched to their Facebook accounts for marketing and to train its algorithms. *Id.* ¶ 56.

The Pixel and related business tools transmitted a wide variety of viewing data to Meta. This included personally identifiable information (PII) about the person watching video. *Id.* ¶ 54. One way it did so was via the Facebook ID (FID), which is a unique and persistent identifier that Facebook assigns to each user. *Id.* Several cookies also work in conjunction with the Pixel that contains the visitor's FID, including the c_user cookie. *Id.* The viewing data also included events like the video's URL whenever a viewer access that webpage, the title of the video watched, when a view started and finished the video's consent, and when the viewer started and finished the advertisement that plays before the video. *Id.* ¶¶ 57–77. The Pixel also scanned form fields containing a user's email, first name, last name, gender, phone number, city, state, and zip code. *Id.* ¶ 65.

Plaintiffs did not consent to Meta obtaining their video viewing data and other internet activities. *Id.* ¶¶ 7–9. Meta's Terms of Service, Data Policy, and Cookies Policy never specifically indicated that Meta may acquire video viewing history obtained from Facebook users' interactions on third-party websites. *Id.* ¶¶ 80–82. None of the subject websites obtained express written consent for the disclosure of video viewing to Meta. *Id.* ¶ 83. Meta also made several false representations and warranties that it does not collect

sensitive information like the information at issue here. *Id.* ¶ 84.

B. Procedural Background

Plaintiffs filed a Class Action Complaint on behalf of everyone in the United States who watched videos on HGTV.com, Bloomberg.com, USAToday.com, 247Sports.com, or PBS.com against Meta Platforms, Inc. FAC ¶ 1. Plaintiffs originally filed in Santa Clara Superior Court. ECF 1 ¶ 1. Plaintiffs then filed their First Amended Complaint (FAC) in Santa Clara Superior Court. *Id.* The FAC alleged six counts under the Federal Wiretap Act, CIPA, and negligence. FAC ¶¶ 112–75. Defendants then properly removed the case to the Northern District of California using federal question jurisdiction. ECF 1 ¶ 6.

Defendants moved to dismiss Plaintiff's FAC under Rule 12(b)(6). ECF 24. Defendants also attached a Request for Judicial Notice in support of its motion to dismiss under Federal Rule of Evidence 201. ECF 24-18. Plaintiffs opposed the motion to dismiss, and Defendant submitted a reply in support of it. ECF 29, ECF 32. Through these pleadings, Plaintiffs withdrew their causes of action brought under the Federal Wiretap Act (Counts I and V) and negligence (Count VI), leaving 3 counts: Counts II, III, and IV, all under CIPA. ECF 29 at 1 n.1. Defendant consequently asserted and provided evidence of the Court's jurisdiction under the Class Action Fairness Act. ECF 36; ECF 45. Plaintiffs did not object. ECF 43. The Court agreed. ECF 48.

II. LEGAL STANDARD

A motion to dismiss for failure to state a claim under Rule 12(b)(6) tests the legal sufficiency of a complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). When reviewing a 12(b)(6) motion, a court "must accept as true all factual allegations in the complaint and draw all reasonable inferences in favor of the non-moving party." *Retail Prop. Trust v. United Bd. of Carpenters & Joiners of Am.*, 768 F.3d 938, 945 (9th Cir. 2014). A court, however, need not accept as true "allegations that are merely conclusory,

unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Secs. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008). A claim is facially plausible when it "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* If a court grants a motion to dismiss, leave to amend should be granted unless the pleading could not possibly be cured by the allegation of other facts. *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000).

III. JUDICIAL NOTICE AND INCORPORATION BY REFERENCE

When ruling on a Rule 12(b)(6) motion, district courts may consider documents attached to the complaint, documents incorporated by reference into the complaint, and matters of judicial notice without converting a motion to dismiss into one for summary judgment. *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003).

Defendant requests that the Court consider Exhibits 1 through 16 when ruling on its motion to dismiss by (1) taking judicial notice of Exhibits 1 through 16 pursuant to Federal Rule of Evidence 201(b), and/or (2) deeming them incorporated by reference. ECF 24-18 at 1. These 16 exhibits encompass Meta's Terms of Service, Meta's Data Policy (now called the Privacy Policy), and Meta's Cookies Policy that were in effect on January 1, 2021, as well as their subsequent versions. *Id.* at 1–3. All exhibits can be found on either Meta's website or on the Internet Archive. *Id.*

A. Judicial Notice

Defendant requests that the Court take judicial notice of Exhibits 1 through 16 pursuant to Federal Rule of Evidence 201 because they are public records available on publicly available websites. ECF 24-18 at 1.

Federal Rule of Evidence 201 allows a court to take judicial notice of "a fact that is not subject to reasonable dispute" because it is "generally known" within the court's jurisdiction or can be "accurately and readily determined from sources whose accuracy cannot be reasonably questioned."

Defendant argues that the Court may take judicial notice of all 16 exhibits under Federal Rule of Evidence 201 because they are "available on publicly available websites

and the contents are not subject to reasonable dispute." ECF 24-18 at 3. The Court agrees. Courts routinely take judicial notice of terms of service and other policies, including content from Internet Archive's Wayback Machine. *Zhang v. Twitter Inc.*, Case No. 23-cv-00980, 2023 WL 5493823, at *3 (N.D. Cal. Aug. 23, 2023). Thus, this Court finds that Exhibits 1 through 16 are judicially noticeable. While the Court will take notice of the existence and contents of Exhibits 1 through 16, it cannot and will not draw other conclusions or inferences. *See In re Meta Tax Filing Cases*, Case No. 22-cv-07557, 2024 WL 1251350, at *3 (N.D. Cal. Mar. 25, 2024).

B. Incorporation by Reference

Defendant additionally requests that the Court deem Exhibits 1 through 16 incorporated by reference. ECF 24-18 at 1. Because the Court judicially noticed all exhibits under Federal Rule of Evidence 201 and will therefore consider them in its Rule 12(b)(6) analysis, it does not find it necessary to determine whether they should also be incorporated by reference.

IV. DISCUSSION

A. Consent

Defendant argues that as a general matter, all of Plaintiffs' claims fail because Plaintiffs consented to Defendant's alleged receipt of their video viewing data. ECF 24 at 7. Defendant reasons that because Plaintiffs consented to Defendant's policies, specifically its Terms of Service, Data Policy, and Cookies Policy, when they signed up for a Facebook account and used Meta's services, and those policies adequately disclose that it would collect data from third-party sites for advertising purposes, Plaintiffs' consent of its policies equated to also consenting to the sharing of their video viewing data. The Court finds that this argument fails because it cannot determine at this stage that Plaintiffs consented to Defendant's policies.

Contracts on the Internet are typically either clickwrap agreements, in which website users are required to click on an "I agree" box after being presented with a list of terms and conditions of use, or browsewrap agreements, where a website's terms and

conditions of use are generally posted on the website via a hyperlink at the bottom of the screen. *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014). While a clickwrap agreement requires the user to manifest assent expressly, a browsewrap contract doesn't require affirmative action. *Id.* Instead, its validity depends on "whether the user has actual or constructive knowledge of a website's terms and conditions." *Id.*

Here, Defendant alleges that Plaintiffs "agreed to Meta's policies by creating a Facebook account and using Meta's services." ECF 24 at 7. There is no evidence in the record that Plaintiffs were required to affirmatively acknowledge the policies before signing up for Facebook that would constitute consent to a clickwrap agreement. Defendant has also not shown that Plaintiffs consented to a browsewrap agreement. While Plaintiffs *could* have given consent "simply by using the website," Defendant has not shown that Plaintiffs had the requisite actual or constructive knowledge of the policies. *See Nguyen*, 763 F.3d at 1176. It is not sufficient to simply allege that the policies exist and Plaintiffs created and used a Facebook account to prove consent. *See In re Meta Tax Filing Cases*, 2024 WL 1251350, at *5. The Court is not persuaded at this time that Plaintiffs consented to Defendant's policies.

Because the Court cannot determine that Plaintiffs have consented to Defendant's policies, the Court does not find it necessary to determine whether consenting to those policies resulted in also consenting to the sharing of video viewing data.

B. Count II – CIPA § 631

CIPA § 631(a) makes it unlawful to use "any machine, instrument or contrivance" to intentionally intercept the content of a communication over any "telegraph or telephone wire, line, cable or instrument," or to read, attempt to read, or learn the "contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable" without the consent of all parties to the communication. Cal. Pen. Code § 631(a). Thus, it is limited to the "contents or meaning" of a communication. *Id*. The Ninth Circuit held that contents "refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of

the message that is generated in the course of the communication." *Gershzon v. Meta Platforms, Inc.*, Case No. 23-cv-00083, 2023 WL 5420234, at *12 (N.D. Cal. Aug. 22, 2023) (citing *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014)). "The analysis for a violation of CIPA is the same as that under the federal Wiretap Act." *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020).

Here, Plaintiffs allege that the unlawful intercepted communications include "detailed URL request[s], form field entries like email address and name, button clicks and associated text, and the title of videos that the subscribers asked the subject websites to deliver." FAC ¶ 119. Defendant argues that none of these communications are contents because they are not "the intended message conveyed," and therefore Plaintiffs fail to state a claim under CIPA § 631. ECF 24 at 12. The Court finds that Plaintiffs have sufficiently alleged that some of the communications are "contents."

1. Detailed URL Request and Title of Videos

Plaintiffs allege that the Pixel intercepted the video's URL, as well as the title of the video watched. FAC ¶¶ 60, 68–69, 74, 77.

To determine whether information is contents, Courts employ a contextual "case-specific" analysis hinging on "how much information would be revealed" by the information's tracking and disclosure. *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1092 (N.D. Cal. 2022). This district further clarified that under CIPA, a URL that simply includes "basic identification and address information" is not content, but a URL disclosing a "search term or similar communication made by the user" could be content. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 795 (N.D. Cal. 2022) (citing *In re Zynga Priv. Litig.*, 750 F.3d at 1106).

Here, both the intercepted URLs and the title of the video watched are contents because they provide "significant information regarding the user's browsing history" and divulge "a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's platform." *Gershzon*, 2023 WL 5420234 at *12 (citing *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 at 596, 605). Plaintiffs allege that

the video viewing history can "shed light on people's interests, politics, artistic tastes." FAC ¶ 87. Further, the URL and video title tells Defendant the exact video users watched, which means Defendant is not limited to making an "educated guess about what [users viewed] on the websites." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *Hammerling*, 615 F. Supp. 3d at 1093.

The alleged URLs also go beyond revealing a general webpage address with basic identification information that would render it record information. They are descriptive of the content. For example, the FAC alleges that the URL not only shows that the user watched a specific video called "Plants for a Shady Landscape," but also that it was within HGTV's outdoor, gardens, and planting and maintenance section. FAC ¶ 60. Thus, the intercepted URLs do not, as Defendant alleges, "merely reflect[] the web pages a person has visited"—it reveals both the "path" and "query string" that user used that concerns the substance of a communication. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 795. It also shows content categories and details that describe the current section of the site. *See In re Google RTB Consumer Priv. Litig.*, Case No. 21-cv-2155, 606 F. Supp. 3d 935, 949 (N.D. Cal. June 13, 2022).

Thus, the alleged intercepted URLs and titles of the videos are content, and the claims stemming from these communications pass the Rule 12(b)(6) challenge.

2. Form Field Entries and Facebook ID

Plaintiffs also allege that form field entries are recorded. FAC ¶ 26. Specifically, they allege that Defendants receive a user's email, first name, last name, gender, phone number, city, state, and zip code from form fields, as well as a visitor's FID. *Id.* ¶¶ 64–65, 68, 71, 74.

"Generally, customer information such as a person's name, address, and subscriber number or identity is record information, but it may be contents when it is part of the substance of the message conveyed to the recipient." *Hammerling*, 615 F. Supp. 3d at 1093 (citing *In re Zynga Priv. Litig.*, 750 F.3d at 1104, 1108–09).

The Court finds that the alleged form fields and FID are "record" information, not

"contents." ECF 24 at 13. They divulge only customer record information such as the user's name, address, and subscriber identity. *See In re Zynga Priv. Litig.*, 750 F.3d at 1106. Further, they are automatically generated in the course of communication—the Pixel and browser are automatically prompted to scan the form fields and transmit the c_user cookie with the FID when a visitor watches a video. *Id.* Thus, they are not user-generated material, just routine identifiers not protected by CIPA § 631. *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082 (C.D. Cal. 2021).

Thus, the form field entries and FID are not contents, and the claims related to these communications do not pass Defendant's Rule 12(b)(6) challenge.

3. Button Clicks and Associated Texts

Plaintiffs also allege that Defendant intercepts button clicks and its associated text. FAC ¶ 119. Specifically, they allege that Defendant intercepts when a viewer starts and finishes the advertisement that plays before the video and the video itself, the names of the buttons, and pages visited as a result of button clicks (including the video's title). FAC ¶¶ 26, 61–63.

User habits are often record information and thus not contents. For example, the Ninth Circuit found that a telephone call's "origination, length, and time" was not contents. *United States v. Reed*, 575 F.3d 900, 917 (9th Cir. 2009). This District also found that usage and engagement data such as installation metrics, number of days users were active, and a user's total time spent on a third-party app was not content. *Hammerling*, 615 F. Supp. 3d at 1093. However, the court emphasized "how much information would be revealed" by the information's tracking and disclosure, stating that had the information intercepted "identif[ied] the specific videos or document that the user view[ed]" would make this data contents. *Id.* at 1092–1093.

Here, generally the alleged button clicks and pages viewed are record information since they are akin to user habits. While the majority of the button click data do not convey the intended message in the same way as, for example, the intercepted URLs, Plaintiffs have also specifically alleged certain button clicks that do. *See Yoon*, 549 F.

Supp. 3d at 1082. For example, they allege that a button click discloses the video's title, which identifies the "specific videos . . . that the user view[ed]," making it content. *Hammerling*, 615 F. Supp. 3d at 1093; *supra* Section IV.B.1. In a similar vein, tracking viewership of the video and knowing what exact video it is, taken together, describes the substance of the communications and is thus contents. These two exceptions allow Defendant to go beyond an "educated guess." *Hammerling*, 615 F. Supp. 3d at 1093.

Thus, the button click data associated with the video titles are contents and pass Defendant's 12(b)(6) challenge. However, the rest of the button click data are not contents and these claims do not pass Defendant's Rule 12(b)(6) challenge.

C. Count III – CIPA § 632

Plaintiffs also allege that Defendant violated California Penal Code § 632 when Defendant used the Pixel to collect confidential video viewing data without prior consent. FAC ¶¶ 142–46. Defendant argues that this claim was not plausibly alleged because the alleged web-browsing data is not "confidential." ECF 24 at 13.

Under CIPA § 632, a communication is confidential if "a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 777 (2002). Courts generally find that Internet communications do not have an objectively reasonable expectation of confidentiality, especially if those communications can be easily shared by the recipients of the communications. *Brown v. Google LLC*, 685 F. Supp. 3d 909, 938 (N.D. Cal. 2023); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014). Plaintiffs must plead "something unique about these particular internet communications" to justify that they are confidential. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 799.

Defendant first argues that Plaintiffs have not alleged that the collected data was "confidential" because they do not bring any plausible claims under the federal Video Privacy Protection Act (VPPA) or its state analogue. ECF 24 at 13. However, it is irrelevant whether Plaintiffs do not or could not plausibly allege that either of those laws apply here—what matters is CIPA § 632's standard of whether there is an "objectively

reasonable expectation that the conversation is being overheard or recorded." Thus, analysis under VPPA or its state analogue is unnecessary.

Defendant then argues that the collected data is not "confidential" because Plaintiffs have not rebutted the Internet presumption. ECF 24 at 14. The Court finds that they have. The reasoning behind the presumption fails here—Plaintiffs' communications have no recipients, and thus Plaintiffs could not reasonably expect that they would be forwarded or otherwise easily shared. *See In re Google Inc.*, No. 13-MD-02430, 2013 WL 5423918, at *22 (N.D. Cal. Sept. 26, 2013) (involving email); *see also People v. Nakai*, 183 Cal.App.4th 499, 518 (2010) (involving an Internet chat). Further, the court in *Brown* clarified that while there is no reasonable expectation of privacy over URLs that only reveal basic identification information, they do over URLs that disclose "the particular document within a website that a person views. *Brown v. Google*, 685 F. Supp. 3d 909, 941 (N.D. Cal. 2023) (citing *Hammerling*, 615 F. Supp. 3d at 1089). The collected data here is therefore confidential because it allegedly reveals the exact title of the video being watched. Plaintiffs' reasonable expectation of privacy is strengthened by the allegation that there was no express written consent for the disclosure of video viewing history and that to the contrary, Defendant made false representations and warranties that it does not collect such information. FAC ¶¶ 83–84; *supra* Section IV.A. Given Defendant's portrayal and Plaintiffs' lack of consent to its collection policies, Plaintiffs could have had a reasonable expectation of privacy over their private browsing. *See Brown*, 685 F. Supp. 3d at 939.

As such, Plaintiffs have plausibly alleged a claim under CIPA § 632 and it passes the Rule 12(b)(6) challenge.

D. Count IV – CIPA § 635

Plaintiffs allege that Defendant violated CIPA § 635 when it implemented the Pixel. FAC ¶¶ 151–52. Defendant argues that there is no private right of action to enforce the statute and that Plaintiffs cannot plead the essential elements of the claim.

1. Private Right of Action

Defendant argues that there is no private right of action to enforce the criminal provisions in CIPA § 635 because Plaintiffs do not allege they were injured by Meta's creation of the Pixel, but rather certain websites' improper use of the Pixel. ECF 24 at 15.

CIPA creates a private right of action for "any person who has been injured by a violation of this chapter." Cal. Penal Code § 637.2(a). "It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages." *Id*. § 637.2(c).

Here, while Defendant is right that Plaintiffs do not allege they were injured by Meta's creation of the Pixel, Plaintiffs *do* allege that they were injured by Meta violating CIPA § 635. ECF 24 at 15; FAC ¶ 154. Thus, unlike *Yoon v. Lululemon*, Plaintiffs allege more than injury from Defendant's use of its tracking devices. *See Yoon*, 549 F. Supp. 3d at 1085. Even if the injury is not direct, this Court has found that "the better interpretation" of CIPA § 637.2 is finding a private right of action for "injuries caused by use of an eavesdropping device are traceable to the manufacture, sale, and provision of that device." *In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d at 1009. As such, because the alleged injuries stemming from the websites' usage of the Pixel were because of Meta's violation of CIPA § 635, there is a private right of action.

Thus, there is a plausible private right of action and it passes the Rule 12(b)(6) challenge.

2. Primarily or Exclusively Designed

Defendant then argues that Plaintiffs have not plausibly alleged a violation of CIPA § 635 because the Pixel cannot be primarily useful for unlawful spying if it is "perfectly lawful when used properly" and is "widely deployed across many industries." ECF 24 at 17–18.

In a Rule 12(b)(6) analysis, the Court must accept as true all factual allegations in the complaint and draw all reasonable inferences in favor of the non-moving party. *Retail Prop. Trust*, 768 F.3d at 945. The question at this stage is "not whether the Court can

imagine any purpose . . . other than eavesdropping but instead whether plaintiffs' allegations are sufficient to plausibly state a claim." *In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d at 1010. Here, Plaintiffs allege that that the Pixel is a "device" that was "primarily or exclusively designed" for eavesdropping because it was designed to gather information about what URLs users visit and what they search for. FAC ¶ 152. They additionally allege that the Pixel is "invisible." FAC ¶ 24. These allegations can still be true, even if it can be used lawfully and is widely deployed. Drawing all reasonable inferences in Plaintiffs' favor, these nonconclusory allegations are sufficient to plead that the Pixel is primarily designed for eavesdropping. *In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d at 1009.

Thus, Plaintiffs sufficiently allege that the Pixel is "primarily or exclusively designed" for eavesdropping and pass the 12(b)(6) challenge.

3. Scienter

Defendant lastly argues that Plaintiffs "allege no facts plausibly showing any such knowledge or intent" as required under CIPA § 635. ECF 24 at 18.

Under CIPA § 635, "[t]he crime lies in intentionally manufacturing the device, knowing that it could be primarily used for wiretapping. The statute does not require intent or knowledge that the device would actually be used unlawfully." *United States v. Christensen*, 828 F.3d 763, 792 (9th Cir. 2015). Intent and knowledge "may be alleged generally." Fed. R. Civ. P. 9(b).

Plaintiffs argue that Meta knew and intended the result of wiretapping by alleging that Defendant's entire business model is based on surveillance and "gunning hard to get lots and lots of third-party data about its users into its database." FAC ¶¶ 12–22. Further, Plaintiffs allege that Defendant already knew that it was receiving video information through its devices. FAC ¶ 87. Thus, because collecting video information would be helpful to Defendant and Defendant knowingly wanted to use that information, the Court finds it is plausible that Defendant knew or intended its surveillance technology to be primarily used for wiretapping. FAC ¶ 92.

However, Defendant argues that Plaintiffs' allegations that the Pixel is widely deployed across many industries and Meta's policies forbid third-party developers from sending any sensitive information shows that Meta did not have knowledge or intent. ECF 24 at 18. That the Pixel is widely deployed is irrelevant to whether it could primarily be used for wiretapping. Further, Defendant's policies limiting the use of the Pixel can show that Defendant knew it could be used for wiretapping if used improperly as it addressed the potential for misuse. CIPA § 635 does not require the intent that the device *would* be used unlawfully, just that it *could* be. *Christensen*, 828 F.3d at 792.

Thus, Plaintiffs have sufficiently alleged scienter and pass the Rule 12(b)(6) challenge.

V. CONCLUSION

Based on the foregoing, the Court GRANTS Defendant's request for judicial notice as to all 16 exhibits. Further, the Court GRANTS Defendant's Rule 12(b)(6) motion to dismiss regarding CIPA § 631 claims stemming from form field entries, FID, and button click data not related to the title of the video and DENIES Defendant's motion to dismiss on all other claims. Because the deficiencies can be remedied, the Court also GRANTS Plaintiffs leave to file a second amended complaint. Plaintiffs must file their amended complaint or notify the Court that they do not wish to amend by January 21, 2025. Plaintiffs may not add any new parties or claims without further leave of Court.

IT IS SO ORDERED.

Dated: December 30, 2024

NATHANAEL M. COUSINS
United States Magistrate Judge